

AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the
District of New HampshireIn the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)INFORMATION ASSOCIATED WITH YAHOO GUID
2HBOGNKXFALZJ2MZHDOYFFV5H4 THAT IS STORED AT
PREMISES CONTROLLED BY OATH HOLDINGS, INC

Case No. 21-mj- 81-01-AJ

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 USC §2252A(a)(1)	Illegal Transportation of Child Pornography
18 USC §2251(a) & (e)	Illegal Production and Attempted Production of Child Pornography

The application is based on these facts:
See the Affidavit of Shawn Serra, SA HSI☒ Continued on the attached sheet.☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Shawn Serra

Applicant's signature

Shawn Serra, SA HSI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
Telephonic conference (specify reliable electronic means).Date: Mar 24, 2021

Judge's signature

City and state: Concord, New Hampshire

Andrea K. Johnstone, US Magistrate Judge

Printed name and title

**UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE**

IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH)
YAHOO GUID)
2HBOGNKXFALZJ2MZHDOYFFV5H4 THAT)
IS STORED AT PREMISES CONTROLLED BY)
OATH HOLDINGS, INC)
_____)

No. 1:21-MJ- 81-01-AJ

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Shawn Serra, a Special Agent with the United States Department of Homeland Security, Immigration and Customs Enforcement (“ICE”), Homeland Security Investigations (“HSI”), being duly sworn, depose and state as follows:

INTRODUCTION

1. I make this affidavit in support of an application for a search warrant for content and records associated with the Yahoo! account identified by the Yahoo! Globally Unique Identifier (GUID) 2HBOGNKXFALZJ2MZHDOYFFV5H4 (hereinafter referred to as the “SUBJECT ACCOUNT”), Oath Holdings Inc. (“Yahoo”), an email provider headquartered at 701 First Avenue, Sunnyvale, California 94089. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Oath Holdings Inc. to disclose to the government copies of the information further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

AGENT BACKGROUND

2. I am a “Federal law enforcement officer” within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

3. Since June 2005, I have served as an HSI Special Agent, and I am currently assigned to HSI Resident Office in Manchester, New Hampshire. As part of my regular duties as a special agent, I investigate criminal violations related to online sexual exploitation of children. I have received training in the areas of child sexual exploitation including, but not limited to, possession, distribution, receipt, and production of child pornography, and interstate travel with intent to engage in criminal sexual activity, by attending a twenty-three-week training program at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia. I am also a member of the New Hampshire Internet Crimes Against Children (ICAC) Task Force, which includes numerous federal, state and local law enforcement agencies, which conducts proactive and reactive investigations involving online child exploitation. In the course of investigating crimes related to the sexual exploitation of children, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in various forms, including, but not limited to, print, video, and digital/computer media.

4. The statements in this affidavit are based on my personal observations, my training and experience, and information obtained from and discussions with other officers. Because this affidavit is being submitted for the limited purpose of securing the requested search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth the facts that I believe are sufficient to support my request.

STATUTORY AUTHORITY

5. This investigation concerns alleged violations of Title 18, United States Code, Sections 2252A(a)(1) and 2251(a) & (e).

a. 18 U.S.C. § 2252A(a)(1) prohibits a person from knowingly transporting any child pornography using any means or facility of interstate commerce or in or affecting interstate or foreign commerce by any means, including by computer.

b. 18 U.S.C. § 2251(a) makes it a crime for any person to employ, use, persuade, induce, entice, or coerce any minor to engage in any sexually explicit conduct for the purpose of producing any visual depiction of such conduct if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, if that visual depiction was produced or transmitted using materials using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or mailed. Subsection (e) of 2251 criminalizes attempts and conspiracies to commit this offense.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that the SUBJECT ACCOUNT has been used to violate, or contains evidence of violations, of 18 U.S.C. §§ 2252A(a)(1) and 2251(a) & (e). There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes, as further described in Attachment B.

7. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711(3) and 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that - has jurisdiction

over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

BACKGROUND ON EMAIL SERVICES

8. In general, an email that is sent to a Yahoo subscriber is stored in the subscriber’s “mail box” on Yahoo’s servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Yahoo servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Yahoo’s servers for a certain period of time.

9. In my training and experience, I have learned that Yahoo provides a variety of on-line services, including electronic mail (“email”) access, to the public. Yahoo allows subscribers to obtain email accounts at the domain name yahoo.com, like the email accounts listed in Attachment A. Subscribers obtain an account by registering with Yahoo. During the registration process, Yahoo asks subscribers to provide basic personal information. Therefore, the computers of Yahoo are likely to contain stored electronic communications (including retrieved and unretrieved email for Yahoo subscribers) and information concerning subscribers and their use of Yahoo services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

10. A Yahoo subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Yahoo. In my training and

experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

11. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

12. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

13. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

14. This application seeks a warrant to search all responsive records and information under the control of Yahoo, a provider subject to the jurisdiction of this court, regardless of where Yahoo has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Yahoo's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

15. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts

lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

BACKGROUND ON CYBERTIPS

16. This Application is part of an investigation initiated by reports or "Cybertips", filed with the National Center for Missing and Exploited Children (NCMEC) and involving the suspected production and possession of child pornography. As used herein, "child pornography" includes visual depictions, such as computer images, of sexually explicit conduct where the production of such visual depiction involves the use of a minor engaging in "sexually explicit conduct" as defined in 18 U.S.C. § 2256(2)(A), all in violation of 18 U.S.C. §§ 2251 and 2252A.

Such conduct includes actual or simulated sexual intercourse of any kind, masturbation, bestiality, sadistic or masochistic behavior, and the lascivious exhibition of the genital or pubic area.

17. NCMEC is a private, nonprofit organization that provides services related to preventing the abduction and sexual exploitation of children. NCMEC does not conduct investigations, but receives reports of child exploitation and makes those reports available to law enforcement agencies for independent review and investigation.

18. Pursuant to Title 18 U.S.C. Section 2258A, a provider of electronic communication services or remote computing services to the public through a means or facility of interstate commerce, such as the Internet, shall report incidents of apparent violations of child exploitation statutes to the CyberTipline. Such reports may include the suspect image and video.

PROBABLE CAUSE

19. On March 10, 2021 Detective Adam Cortese of the Manchester Police Department (MPD) received a notification from his ICAC account that there had been two Cybertips assigned to the MPD. The Cybertips came from NCMEC and were identified as Cybertip numbers 87448815 and 87517835. The tips were linked together reporting on the same suspect accounts. The tips were received by NCMEC on March 08, 2021 and March 10, 2021 respectively from Yahoo! Inc. and reported that the Yahoo! account with the Globally Unique Identifier (GUID) 2HBOGNKXFALZJ2MZHDOYFFV5H4 had been identified as sending 30 emails containing 359 files of possible Child Sexual Abuse Images (CSAI) from the email account bostonpapi1985@gmail.com to the email account bostonpapi1985@gmail.com.

20. Yahoo! provided the following information associated with the suspect account:
- a. Name: Randy Taylor
 - b. User ID: 2HBOGNKXFALZJ2MZHDOYFFV5H4

- c. Recovery/ Alternate Email Address: bostonpapi1985@gmail.com (SUBJECT ACCOUNT).

21. On March 16, 2021, Detective Cortese served Yahoo! Inc. a preservation request for the SUBJECT ACCOUNT. In general, an email that is sent to a Yahoo subscriber is stored in the subscriber's "mail box" on Yahoo servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Yahoo servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Yahoo's servers for a certain period of time.

22. On March 18, 2021, your affiant spoke with representatives of Verizon Media (Yahoo's parent company) and learned that Yahoo! users have the ability to manage third-party email accounts, such as Gmail accounts, through their Yahoo! account by linking the third-party account to their Yahoo! account. By linking other email accounts, users are able to send and receive emails from multiple accounts from within their Yahoo! account. Your affiant was further advised that email "sent events" are scanned for child sexual abuse material. These events can occur across email accounts if the accounts are merged into one mail repository or if the email is accessed through the Yahoo! account.

23. As part of the aforementioned Cybertips, Yahoo! sent NCMEC 359 files sent by the suspect account. All of the files had been reviewed by workers from Yahoo! and they believed them to be CSAI. The employees from Yahoo! also identified EXIF data in some of the photos, including GPS coordinates and camera device information, that suggested the suspect was producing some of the images. Your affiant is aware from training and experience that EXIF, or Exchangeable Image File Format, data is a standard storage format for camera and

image metadata in JPEG and TIFF files. EXIF data may include the camera make and model that took a picture, and GPS coordinates of where the picture was taken.

24. Detective Cortese reviewed the files included with the Cybertips and observed what appeared to be voyeur-style photos of minors in the shower or in various stages of undress. Accordingly, none of the female subjects in the photos appear to be aware of the camera. Some of the files had been merged to create collages focused on the genitals or breasts of the minors. Descriptions of 6 of the files are as follows:

- a. Original Filename: IMG-0007.jpg- A photo of a naked prepubescent girl about 10-12 years old standing in the shower with one leg raised to step out of the shower. Her vagina and buttocks are exposed to the camera.
- b. Original Filename: IMG-6152.jpg- A photo of a naked prepubescent girl about 10-12 years old standing in the shower. Her vagina is exposed to the camera. This appeared to be the same juvenile female as in IMG-0007.jpg
- c. Original Filename: IMG-0212.jpg- A photo of a pubescent girl about 13-16 years old sitting on the toilet with her shorts around her knees. She is topless so that her breasts are exposed to the camera.
- d. Original Filename: 1581195714820_IMG-0210.jpg- A photo of a pubescent girl about 13-16 years old sitting on the toilet with her shorts around her knees. She is pulling her shirt off over her head so that her breasts are exposed to the camera. This appears to be the same juvenile female as in IMG-0212.jpg.
- e. Original Filename: inCollage_20201212_140109091.jpg- A collage containing 8 photos. The first photo shows an adult male lying on a bed with his penis exposed behind the buttocks of a female wearing black underwear. The female is only

visible from hip to mid-thigh and is not identifiable. Half of the man's face and a section of his torso are visible. He appears to have tattoos on his right arm, chest and stomach. The second photo shows a female child about 9-12 years old lying on a bed. The photo is taken so that the camera can see up her shorts exposing her buttocks. Her buttocks are the focus of the picture and she is only shown from shoulder to mid-thigh. The third photo appears to be a cropped section of 1581195714820_IMG-0210.jpg described above so that the girl is only visible from waist to neck and her breasts are the focus of the photo. The fourth photo appears to be a cropped section of IMG-0007 described above showing the girl from neck to mid-thigh so that her vagina and buttocks are the focus of the picture. The fifth photo is another photo of the same girl in the shower also cropped to show her from neck to just below the groin so that her vagina is the focus of the photo. The sixth photo is a cropped section of IMG-0212.jpg described above to show the girl from her stomach to her neck so that her breasts are the focus of the photo. The seventh photo shows another girl about 11-13 years old laying on a bed on her side. She is wearing short shorts so that her buttocks are slightly exposed. The photo shows her from knee to shoulder and her buttocks are the focus of the photo. The eighth photo is a close-up photo of a vagina and anus. A man's hand can be seen pushing on one of the buttocks to expose the anus. The vagina and anus appear to belong to a minor due to the comparative size to the man's hand and lack of pubic hair, but positive identification as a minor is not possible due to the extreme close-up nature of the photo.

- f. Original Filename: CollageMaker_20201119_201219175.jpg- A collage of 5 photos including a picture of the same man in bed with the same woman as in inCollage_20201212_140109091.jpg, described above. The man's face is clearly visible in this photo.

25. Yahoo! reported that an image from one of the emails included a photo of a New Hampshire driver's license belonging to Randy Taylor, date of birth July 11, 1985 and address 466 Hanover Street, Apt 2, Manchester, NH, 03104.

26. Detective Cortese found a booking photo of Taylor in the MPD database. Using that photo, Detective Cortese was able to identify Taylor as the male in the image named CollageMaker_20201119_201219175.jpg, Original Filename: inCollage_20201212_140109091.jpg. Through further investigation, Detective Cortese determined that Taylor's current home address was 10 Hillcrest Ave, Manchester NH 03103.

27. On March 16, 2021, your affiant learned of the investigation and was provided copies of the Cybertips, a copy of the search warrant executed at Taylor's residence, and the MPD reports.

28. This application seeks a warrant to search all responsive records and information under the control of Yahoo, a provider subject to the jurisdiction of this court, regardless of where has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Yahoo's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.

29. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

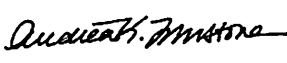
30. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Yahoo, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

/s/ Shawn Serra
Shawn Serra
Special Agent
Homeland Security Investigations

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: Mar 24, 2021
Time: 5:05 PM, Mar 24, 2021



Andrea K. Johnstone
U.S. Magistrate Judge



ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

This warrant applies to information associated with Yahoo! GUID **2HBOGNKXFALZJ2MZHDOYFFV5H4**, as well as data preserved from that account pursuant to a preservation request made on March 16, 2021, that is stored at premises owned, maintained, controlled or operated by Oath Holdings, Inc. (“Yahoo”), an email provider that accepts service of legal process at 701 First Avenue, Sunnyvale, California 94089.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Oath Holdings, Inc/Yahoo (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on March 16, 2021, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account from January 1, 2019 to the present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within fourteen days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(1) and 2251(a) & (e), those violations involving the user of the Yahoo! GUID 2HBOGNKXFALZJ2MZHDOYFFV5H4 and others unknown occurring on or after January 1, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) Communications regarding the production, receipt, and possession of child pornography.
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used GUID 2HBOGNKXFALZJ2MZHDOYFFV5H4, including records that help reveal the whereabouts of such person(s);
- (e) The identity of the person(s) who communicated with the user of GUID 2HBOGNKXFALZJ2MZHDOYFFV5H4 about the production, receipt, and possession of child pornography, including records that help reveal their whereabouts.